2011-05

Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses

Hart, Steven

Monterey, California. Naval Postgraduate School

A Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses

Steven Hart and Jim Ramsay

ABSTRACT

Over 350 academic programs in the United States currently offer instruction in the field of homeland defense and security. In spite of this growth at the program level over the past ten years, there still exists a shortage of instructors and coursework in critical infrastructure protection (CIP). Traditional instructor preparation (which is accomplished through the attainment of an advanced degree coupled with research and professional experience) does not currently produce enough instructors qualified in CIP because of the extremely limited number of CIP-related educational opportunities. Therefore, an alternate venue for instructor preparation must be provided. This article addresses that need by providing a guide for educators who desire to engage in a deliberate self-study program to develop sufficient expertise to teach a first course in physical CIP at the undergraduate or master's degree level. This information is also useful for professionals who have had to assume CIP-related duties and functions without the benefit of supporting coursework. This article introduces a five-part framework for understanding CIP – policy, networks, level of hazard, level of protection, and system design – and provides resources for understanding each part of the framework. Each element of the framework is introduced and briefly explained and then resources are presented which will allow the reader to explore this particular topic in detail. Where possible, resources are presented as web links to allow the reader to directly access the learning resource, free of charge. The article concludes with guidance for adapting the five-part framework and the materials presented in designing a CIP course tailored to the needs of a specific instructor and institution.

INTRODUCTION

Over the past fifty years, as societies became more interconnected and interdependent, our government recognized the importance of protecting the infrastructures that are essential to the functioning of the nation. In 1963, President Kennedy established the National Communications System (NCS) to ensure the federal government's ability to communicate in emergency situations including nuclear attack. In 1979, the Federal Emergency Management Agency (FEMA) was established with responsibilities including civil defense and hurricane and earthquake risk reduction. In the 1980s, our current understanding of critical infrastructure began to evolve when President Reagan, in an executive order, charged the head of each federal department and agency with the responsibility of protecting essential resources and facilities within their organizations.[1]

The first World Trade Center bombing (1993) and the bombing of the Murrah Federal Building in Oklahoma City (1995) in the continental United States, together with the Sarin gas attack in a Tokyo subway (1995), the bombings of the Nairobi, Kenya and Dar es Salaam, Tanzania embassies (1998), and the small boat attack on the USS Cole (2000) all served to raise the awareness of acts of terror within the American people and government. Concurrent with these events, policy decisions were made by the federal government, which began a coordinated effort to protect critical infrastructures. In 1996, President Clinton established the Presidential Commission on Critical Infrastructure Protection. The work of the commission resulted in the definition of eight critical infrastructure sectors in Presidential Decision Directive 63 (PDD63) in 1998.[2]

The events of September 11, 2001 brought about a rapid expansion of critical

infrastructure protection efforts. The first *National Strategy for Homeland Security* was published in 2002 and was followed by the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and Homeland Security Presidential Directive 7, which replaced PDD63, in 2003. These documents expanded critical infrastructure to thirteen sectors and added five key resources and led to the publication of the first National Infrastructure Protection Plan (NIPP) in 2006, with the second edition following in 2009. Currently, the NIPP defines Critical Infrastructure as:[3]

> Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

The eighteen Critical Infrastructure and Key Resource (CIKR) sectors are defined as:

Agriculture and Food	Water	Nuclear Reactors
Defense Industrial Base	Chemical	Information Technology
Energy	Commercial Facilities	Communications
Healthcare and Public Health	Critical Manufacturing	Postal & Shipping
National Monuments & Icons	Dams	Transportation Systems
Banking and Finance	Emergency Services	Government Facilities

Each CIKR sector and specific components in each sector have physical, human, and cyber elements. The proportion of these elements and the associated vulnerabilities vary between sectors. Some sectors such as water, energy, and government facilities rely heavily on physical elements while others – like banking and finance, information technology, and communications – have predominately cyber elements.

This article provides recommendations to educators and professionals who desire to increase their knowledge, skills, and abilities in the protection of physical critical infrastructure elements for the purpose of developing or improving courses in critical infrastructure protection (CIP). The focus of this paper is on physical and human elements that predominate in sectors such as water, energy, government facilities, critical manufacturing, and dams. The principles and concepts also extend to the physical elements of predominately cyber and human infrastructures like information technology, communications, and banking and finance.

Rather than being simply a literature review, this article points to selected elements of the literature and best practices to enable a prospective CIP instructor to gain a basic understanding of the fundamental aspects of CIP. Each section begins with learning objectives and then provides suggested resources for mastering these objectives. The endnote references contain live links so the source documents can be directly accessed from the article. Each section concludes with a statement of what the reader should be able to accomplish after studying the recommended documents and resources. A disciplined application of this program of study will provide the knowledge, skills, and abilities to develop and teach a CIP course appropriately flavored by the instructor's expertise and the institutions goals.

In addition to educators, another group that can benefit from this article are professionals who have had to assume CIP related duties and functions without the benefit of supporting education and training. This document provides an outline for a self-directed course in the physical and human aspects of critical infrastructure protection. A disciplined application of this program of study will enable the reader to better perform CIP-related duties as they pertain to the physical and human dimensions.

SAMPLE CIP PROGRAMS AND RESOURCES AROUND THE NATION

The prospective CIP instructor should begin by reviewing existing programs teaching critical infrastructure protection. This is not done to copy someone else's program, but rather to develop a more comprehensive understanding of the depth, breadth, and focus of existing CIP courses and programs. Additionally, understanding the broader body of work enables an instructor to decide which of the many aspects of CIP are appropriate for in-depth study and inclusion in a particular program's course work. To that end, this section describes the content and location of many of the more notable CIP programs.

The Center for Homeland Defense and Security (CHDS) is located in Monterey, CA and is jointly sponsored by the Naval Postgraduate School (NPS) and FEMA's National Preparedness Directorate. In operation since 2002, the CHDS mission is "To strengthen the national security of the United States by providing graduate level educational programs and services that meet the immediate and long-term leadership needs of organizations responsible for homeland defense and security" and the center provides both master degrees and executive education programs in homeland security.[4] CHDS also provides substantial resources to anyone engaging in professional self-development or developing a CIP course, most notably through the University and Agency Partnership Initiative and Homeland Security Self-Study Courses, which operate in a password-protected secure environment.

The University and Agency Partnership Initiative (UAPI) provides contact information for 209 programs offering educational programs in homeland security and defense. This portal provides access to a wealth of resources including recorded lectures, instructor guides, and upcoming homeland security education conferences. Recommended courses and course content for graduate and undergraduate homeland security education programs are also posted here. The site contains presentations from the Homeland Security and Education Summit held annually for the past four years. These presentations contain information on how educators from all over the country are teaching homeland security.[5]

The Homeland Security Self-Study Course section contains over thirty courses from schools in the UAPI that can be accessed by UAPI members. This information ranges from fully interactive web-based instruction to outlines of course content. The material can be used for self-study by prospective instructors, guidelines for course development, and supplemental material in coursework. Five of the courses available from NPS through this portal provide certificates of completion that can be used to satisfy continuing professional development requirements for certain professions and credential instructors.[6]

The "Resources" tab on the CHDS homepage contains a link to the Homeland Security Digital Library, an electronic collection of documents related to homeland security policy, strategy, management, and operations. As of this writing, it contains over 73,200 items, about half of which require an authenticated login.[7] Other information available includes lectures, software, leader viewpoints, and the current Homeland Security Book List.[8] The philosophy of CHDS is clearly one of easy access to shared information and this is an essential resource in researching, learning, and teaching CIP.

Another excellent source of information and different perspectives is the Critical Infrastructure Protection Program (CIP Program) at George Mason University (GMU). The CIP Program is sponsored by the National Institute of Standards and Technology (NIST) and the Department of Commerce and is located in GMU's School of Law. The CIP Program conducts core research on CIP issues funded by the NIST grant and externally funded research on infrastructure vulnerability, risk mitigation, and infrastructure resilience. Much of the research is archived and available on the website. Another excellent resource available through GMU's CIP Program is *The CIP Report*, a monthly electronic publication containing short articles by researchers, practitioners, and foundations on a variety of infrastructure-related topics. Back issues are archived so the evolution of CIP related

issues can be studied. Like CHDS, the GMU CIP Program maintains an electronic library of selected publications, government documents, and government reports on CIP related issues.[9]

In contrast to the broad, policy-focused educational mission of the Center for Homeland Defense and Security and the research focus of the Critical Infrastructure Protection Program at George Mason University, the Center for Infrastructure Protection and Physical Security (CIPPS) focuses on the architecture, engineering, and design of protective structures. CIPPS resides in the University of Florida's Department of Civil and Coastal Engineering and is led by Dr. Ted Krauthammer, a noted researcher and designer in the realm of blast resistant construction. CIPPS is an engineering center within an engineering school that is concerned with issues of progressive collapse of large structures, software development, and the response of material and structures to explosives loading.[10] CIPPS also sponsors a weeklong short course on the design of modern protective structures based on Dr. Krauthammer's book of the same name.[11]

Two other infrastructure-related university programs bear mentioning. First, the Institute for Crisis, Disaster, and Risk Management at The George Washington University provides education and research in the areas of crisis, emergency, and risk management.[12] Second, Carleton University in Ottawa, Ontario, Canada established, in 2010, a Master of Infrastructure Protection and International Security program. This is a joint project between the Norman Paterson School of International Affairs and the Department of Civil and Environmental Engineering with both faculties providing instruction and leadership. This promises to be a unique program and may set a standard for multi-disciplinary education in this inherently multi-disciplinary field.[13]

A review of these academic programs demonstrates the complexity and variety of approaches currently taken with regard to CIP. After reviewing these programs, the prospective CIP instructor can see the different approaches of selected institutions to the complex fields of homeland defense and security and CIP education.

A CONCEPTUAL FRAMEWORK CIP

A review of these programs can leave a potential instructor overwhelmed with the amount of information available and struggling to process it all. One of the critical pieces of information that may not be readily apparent is a conceptual framework for organizing, relating, and understanding all of the information discovered in such a review. Accordingly, the following five-part conceptual framework, graphically illustrated in Figure 1, is suggested as a tool for mentally organizing and relating CIP information. To borrow a mathematical term, each concept is necessary, but not sufficient, for an overall understanding of CIP.

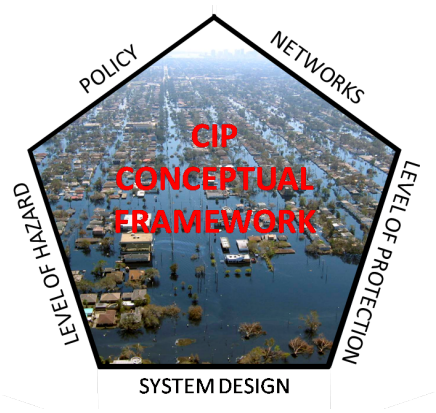

Figure 1. CIP Conceptual Framework

Information encountered during this review process can typically be placed in one of these five categories, as will be demonstrated in the following sections. Additionally, this conceptual framework can also be used to frame the objectives for an introductory CIP course. Using the framework as a tool for self-development and for subsequent course design ensures that instructor preparation is tightly linked to classroom instruction. The program of study proposed in this article is organized around the five concepts in this conceptual framework.

The CIP conceptual framework is rendered as sample course objectives in Figure 2. As is appropriate for an introductory course, these

are at the lower three levels of Bloom's taxonomy: knowledge, comprehension, and application.[14] Achievement of these objectives results in a student who understands and can apply the basic principles of CIP and is prepared to explore specific topics in greater depth.

1. Explain national strategies and policies on infrastructure protection.
2. Identify critical components of a complex infrastructure network.
3. Describe the All Hazards Environment for those critical components.
4. Specify the level of protection or resiliency for those critical components.
5. Describe systems design concepts to achieve the desired protection and resiliency.

Figure 2. CIP Conceptual Framework Rendered as Course Objectives

POLICY

Investigation into the CIP conceptual framework begins with the policy, strategy, plans, and laws that establish the operating environment within which all CIP activities take place. The best place to start is with the two hour IS-860.a National Infrastructure Protection Plan (NIPP) on-line correspondence course offered by FEMA's Emergency Management Institute (http://www.training.fema.gov/). FEMA's IS-860a course offers an overview of the NIPP, which provides the structure and procedures for implementing protection and resiliency of critical infrastructure and key resources.[15] This course on the NIPP does not start at the highest level of policy, but it provides a basic understanding of the implementing document for infrastructure policy. After completing this course, read the documents that led to the development of the NIPP and place it in a broader national context. Starting with the implementing law, this process flows through policy to strategy to subordinate strategies to implementing plans.

Simply put, a law is the authority to do something and the law that leads to all our efforts in CIP is the Homeland Security Act of 2002. This law establishes and organizes the Department of Homeland Security, including its subordinate directorates. It also establishes a framework for the sharing, protection, and dissemination of critical infrastructure information.[16] Most of the agencies and departments working on CIP issues trace their origin to this law.

Homeland Security Presidential Directives (HSPD) are the documents that establish national policy. Of these, HSPD 7, *Critical Infrastructure Identification, Prioritization, and Protection*, is essential to understanding CIP. HSPD 7 "establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." This document establishes policy, assigns roles and responsibilities to DHS, sector-specific federal agencies, and other departments, agencies, and offices and concludes with implementation guidance.[17] Also related to overall CIP efforts are HSPD 8, *National Preparedness*, which requires establishing a national domestic all-hazards preparedness goal and improves federal, state, local, and tribal preparedness coordination,[18] and HSPD 5, *Management of Domestic Incidents*, which establishes the Nation Incident Management System.[19] A list of all HSPD with links to the complete documents is available on the DHS website at http://www.dhs.gov/xabout/laws/editorial_0607.shtm.

From policy flows strategy, which may be defined as the direction and coordination of all national resources to achieve a national policy. *The National Strategy for Homeland Security*, most recently published in October 2007, defines the hazardous environment currently facing the country and establishes the strategic objectives to prevent terrorist

attacks, protect people and critical infrastructure, and respond to and recover from incidents.[20] Within this framework, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, most recently published in February 2003, promulgates national policy, guiding principles, and organization for protecting critical infrastructure. This document additionally addresses the partnerships necessary between government, industry, and citizens to implement the strategy.[21]

Conceptually, the NIPP follows from *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and implements the policies described therein. In implementing the NIPP, each critical infrastructure sector develops a sector specific plan that implements the NIPP risk management framework. The current versions of the thirteen published sector-specific plans are available on the DHS website.[22] Potential instructors should review these plans to see how the NIPP risk management framework has been implemented under different conditions.

Organizationally, the NIPP follows from *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Noting the most recent publication dates of these three documents highlights a critical issue that complicates trying to understand their relationships. These documents are politically driven and change with the political climate and leadership. The process, however, is sometimes slow, and is often non-linear. The first NIPP, published in 2006, implemented *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* as published in 2003, which was developed from the 2002 version of *The National Strategy for Homeland Security*. The current *National Strategy for Homeland Security* was published in 2007 under the previous presidential administration and the current NIPP in 2009 – while an updated version of *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* – has yet to be published. These politically driven changes can lead to discontinuities between the documents and a reader should bear in mind the document publication dates.

Taking the IS-860.a correspondence course and studying these documents will provide a potential CIP instructor a sufficient depth of knowledge to teach an introduction to CIP policy. This depth of knowledge is sufficient for an introductory CIP course, but other resources are available for those instructors and programs seeking greater depth in protection policy and its relationship to emergency management. For institutions focused at the regional or state level, instructors will certainly review regional or state planning documents. As a prospective CIP instructor seeks to expand his or her expertise, the next two documents of interest are most likely the National Response Framework (NRF) which "presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies - from the smallest incident to the largest catastrophe[23] and the National Incident Management System (NIMS) which implements the NRF across all levels of government in the all-hazards environment.[24] Fortunately, FEMA's EMI has two correspondence courses introducing these two documents. The three-hour IS-800.b National Response Framework, An Introduction course is available at http://training.fema.gov/EMIWeb/IS/IS800b.asp and the three-hour IS-700.a National Incident Management System (NIMS), An Introduction course is at http://www.training.fema.gov/EMIWeb/IS/is700a.asp.

NETWORKS

Most critical infrastructures are networks that are intra-dependent on critical assets within the network and inter-dependent on elements of other critical infrastructures. These interconnected infrastructures behave as networks according to certain principles and these principles can reveal how the network will behave when degraded by random events or deliberate attack. Potential CIP instructors must understand network behavior to determine the critical assets in any system and the critical connections between systems. This section provides

resources to enable potential CIP instructors to develop this understanding.

Much of theory that relates to infrastructure networks is based on the work of Albert László Barabási. An excellent primer is available in the article "Scale-Free Networks" (published in *Scientific American*) [25] which explains the basic concepts and behaviors of different types of networks and how these concepts apply to infrastructure. A more rigorous treatment of medium length on the topic is "The Structure and Function of Complex Networks" by M.E.J. Newman [26] from 2003. This article explains network analysis in mathematical terms and its application to social, information, technological, and biological networks. The article uses the work of Barabási but also explains its shortcomings in some applications and considers the work of other network researchers.

Dr. Ted G. Lewis applies these concepts of network analysis to the field of critical infrastructure protection in his textbook *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.*[27] The book, which resulted from the development of a course on this topic at the Naval Postgraduate School, presents a scientific treatment of infrastructure networks and provides tools to assess the vulnerability of these networks. An on-line version of this course and selected topics from the textbook is available through the Center for Homeland Defense and Security Homeland Security Self Study Course section previously discussed.

Upon reading these two articles and completing this course, the prospective CIP instructor will be able to describe the principles of network science, explain the behavior of an infrastructure network according to these principles, and determine the critical elements within an infrastructure network. For the potential instructor who desires a deeper understanding of network science or additional network tools the following resources are suggested.

The Center for Computational Analysis of Social and Organizational Systems (CASOS) is a university wide center at Carnegie Mellon University conducting multi-disciplinary research on network dynamics. From this site, a free software package called ORA (Organizational Risk Analyzer) can be downloaded. ORA is designed for social network analysis but is readily adaptable for analyzing inter- and intra-dependencies of infrastructures. ORA provides statistical tools for network analysis, network visualization tools including an option for geospatial visualization, and time based change detection.[28] Additionally, the Interdisciplinary Center for Network Science and Application at the University of Norte Dame addresses network science problems in social, biological, organizational, technical, and defense systems. The webpage contains an extensive list of links to network related publications.[29]

Each of these resources provides information on how to analyze networks, but not on where or how to collect the network data to be analyzed. One source of nationwide infrastructure data is the DHS Integrated Common Analysis Viewer (iCAV), a web based, secure, geospatial visualization tool that provides access to 400 infrastructure data layers, population information, weather information, and analysis tools. It is useful for providing data for analysis in other programs such as ORA, situational awareness, and emergency response. Access is through the Homeland Security Information Network (HSIN), and HSIN accounts are available through the DHS website.[30] Clicking the link in the footnote will take one to the appropriate page to request HSIN and iCAV access.

LEVEL OF HAZARD - LEVEL OF PROTECTION

At this point a prospective CIP instructor understands national and regional policy on infrastructure protection and is able to identify the critical elements within an infrastructure network. With this knowledge, the next questions are obvious, "What can go wrong with those critical elements and what should be done about it?" While the questions may be phrased and investigated separately, they are linked through the risk management process. Investigation of this process begins with understanding these key definitions.

> **Risk:** The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequence.[31]
>
> **Risk Analysis:** The process of determining relative levels of risk for a group of assets, generally a function of threat likelihood, asset value, and consequence.[32]
>
> **Risk Management:** The process of evaluating how changes in applied countermeasures affect risk levels and costs for the purpose of decision making.[33]

When considering risk, the undesirable outcomes are described in the All Hazards Environment. To consideration of threats and hazards, risk analysis adds consideration of the value of the asset and the consequence of its loss or damage to determine a relative level of risk. Then appropriate levels of protection considering cost and acceptable risk are selected through an appropriate risk management procedure. In studying the following resources, the prospective CIP instructor develops the ability to balance the level of hazard with an appropriate level of protection through the risk management process.

THE ALL HAZARDS ENVIRONMENT

The NIPP defines the All Hazards Environment as "a grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects."[34] One way to make this more manageable is to consider terrorism, earth effects and natural disasters, accidents, and deterioration individually. Since terrorism and earth effects and natural disasters have been the areas of greatest concern and most recent research, they will be discussed in detail here. Accidents and deterioration are currently best studied through current events. It may be that recent events such as the I-35 bridge collapse and the Deepwater Horizons explosion (BP oil spill in the Gulf of Mexico) and resulting oil leak lead to the establishment of centers to study these issues.

TERRORISM

The impact of terrorism has been a driving force in the need for improving critical infrastructure protection, but the threat of terrorism is not new. Many would agree with the statement that, "the complexity of the modern world and the intricacy of international relations allow guerrilla warfare to be drawn out by new methods of deceit and subversion. In many causes the use of terrorism is regarded as a new way to wage war." However, most would be surprised that the source of this quotation is the Second Vatican Council in 1965[35]. While large-scale terrorism may be a relatively new phenomenon for the United States, other areas of the world have been dealing with it for many years. For the prospective CIP instructor, several references are useful in gaining both a historical and current understanding of this "new way to wage war."

One starting point is *A Military Guide to Terrorism in the Twenty-First Century*. Though published for the U.S. Army, it is useful to anyone interested in terrorism and provides a concise summary for understanding it. The *Guide* is an overview document describing terrorist behavior, motivation, and operations that is supported by six supplements.[36] Supplement 1, *Terror Operations: Case Studies in Terrorism*, contains descriptions and assessments of six terrorist incidents: the Tokyo subway sarin attack, the Murrah Federal Building bombing, the Khobar Towers bombing, the USS Cole bombing, the July 7, 2005 London bombings, and the Beslan hostage crisis and mass murder.[37] Supplement 2, *Critical Infrastructure Threats and Terrorism*, examines the history of critical infrastructure protection and provides guidance in assessing threats to critical infrastructure.[38] These documents, along with the other supplements, are readily available on line.

The U.S. government maintains several terrorism information and intelligence resources available on line that provide up to date information on terrorist activity. The U.S. Department of State Office of the Coordinator for Counterterrorism coordinates government policies and programs aimed at countering terrorism overseas. This office produces and maintains on line the congressionally mandated *Country Reports on Terrorism*, which, in 2004, replaced the previously published *Patterns of Global Terrorism*.[39] The Federal Bureau of Investigation (FBI) maintains a counterterrorism homepage that contains information on the most-wanted terrorists, worldwide threats, and terrorism investigations.[40] The National Counterterrorism Center (NCTC), in operation since 2004, operates under the Office of the Director of National Intelligence and is responsible for threat analysis and information sharing. From their website, the Worldwide Incidents Tracking System (WITS) can be accessed. The WITS is a searchable and sortable database that also has a mapping capability enabling a user to plot terrorist events based on a variety of criteria. Publications, including the *NCTC Report on Terrorism* and the *Intelligence Guide for First Responders* are available on the website.[41] While much of the counterterrorism work of the Central Intelligence Agency is classified, unclassified extracts are available at the Center for the Study of Intelligence along with information on relations with academic institutions.[42]

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a DHS center of excellence based at the University of Maryland. START research is focused in three areas: terrorist group formation and recruitment, terrorist group persistence and dynamics, and societal responses to terrorist threats and attacks. One very useful tool on the START website, www.start.umd.edu/start/, is the Global Terrorism Database (GTD). The GTD is an open-source searchable database containing information on over 80,000 cases from 1970 to 2010 with the most recent update posted July 2, 2010. Another useful tool is the Terrorist Organization Profiles, a searchable database of 800 terrorist organizations last updated on March 1, 2008. Both of these databases were created by the Memorial Institute for the Prevention of Terrorism but are now being managed by START.[43]

The Memorial Institute for the Prevention of Terrorism (MIPT) has its origins in the responses to the 1995 attack on the Alfred P. Murrah Federal Building in Oklahoma City. It began operations in 2000 and is a non-profit organization focused on preventing terrorism through research, knowledge bases, and training. MIPT is supported by the FEMA National Preparedness Directorate, Training Division and provides counter-terrorism training to the Nation's 850,000 uniformed law enforcement officers. MIPT Lawson Library consists of the Terrorism Resource Guide, a series of links to terrorism data bases, studies and reports, and counter-terrorism foundations; the Law Enforcement Guide, an extensive collection of intelligence and policing resources; and the Open Access Journals and Magazines section, links to open access, professional intelligence, homeland security, and law enforcement publications.[44]

The Combating Terrorism Center (CTC) at West Point conducts educational programs and scholarly research on terrorist threats facing the United States. Their educational programs have served the Fire Department of New York and the FBI. Each month, the CTC publishes the *CTC Sentinel* electronic newsletter to disseminate research, contemporary threat analysis, and recent terrorist activities. The *CTC Sentinel* and other research, links, and resources is available on the CTC's website.[45]

After studying these sources, the prospective CIP instructor can describe the historical impact and development of terrorism, describe current trends, tactics, and targets of terrorism, and use terrorism databases in support of education and research. While terrorist events can be very devastating, they are extremely unlikely when compared to natural events that are more common, and can cause greater human and economic dislocation.

EARTH EFFECTS AND NATURAL DISASTERS

Most individuals, communities, and regions are much more likely to deal with earth

effects and natural disasters than they are with terrorism. Unlike terrorism, earth effects and natural disasters can be modeled probabilistically based on over 100 years of collected data. Several resources are available to assist potential CIP instructors in understanding and describing the hazards posed by earth effects and natural disasters several centers are currently involved in mitigation of these hazards.

The principal source of data on earth effects and natural disasters is the United States Geological Survey (USGS) whose website contains specific information on earthquakes, floods, hurricanes, landslides, tsunamis, volcanoes, and wildfires. Fact sheets, disaster trends, engineering design data, and current, real-time hazards are available within each of these categories.[46] For example, a fact sheet on flood hazards, flow estimates for rivers in Tennessee, an explanation of the term "100 year flood," and *Large Floods in the United States: Where They Happen and Why* can all be found in the flood hazard section.[47] Similar information is available for the other earth effects. Also available is the Natural Hazards Support System, which reports real-time data on current natural hazard events. Sample output from this system collected on June 1, 2010 is shown in Figure 3.[48] While the USGS specifies hazards, other resources must be accessed to describe and understand mitigation efforts.

The Natural Hazards Center (NHC) at the University of Colorado at Boulder focuses on

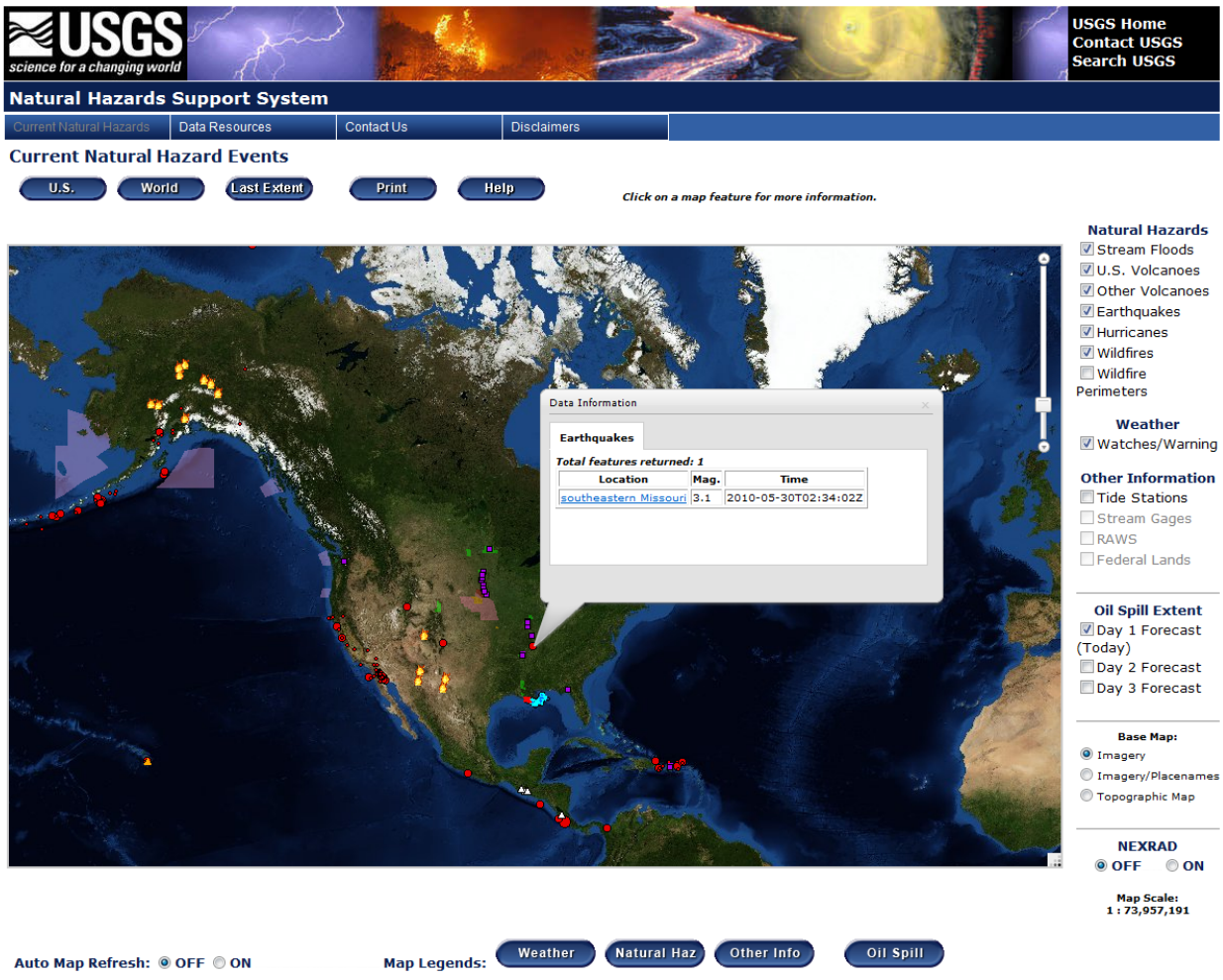

Figure 3. Natural Hazard Support System Screenshot Captured June 1, 2010

the social science and policy aspects of hazard mitigation and disaster preparedness, response, and recovery. The NHC supports a wide variety of research and publications, much of which is available on their website.[49] The Department of Homeland Security Center of Excellence – Natural Disaster, Costal Infrastructure, and Emergency Management (DIEM) is headquartered at the University of North Carolina at Chapel Hill with partners from nineteen other institutions. The DIEM focuses on four areas: Costal Hazard Modeling, Engineering Resilience in the Built and Natural Environments, Disaster Response and Social Resilience, and Resilience Planning. DIEM research available on their website includes the Deepwater Horizons oil spill, Haiti and Chile Earthquakes, and the Hazard Research Colloquia Series.[50] The National Science Foundation supports three earthquake engineering research centers: the Pacific Earthquake Engineering Research Center (PEER) led by the University of California, Berkeley,[51] the Multidisciplinary Center for Earthquake Engineering Research (MCEER) headed by the University of Buffalo, The State University of New York,[52] and the Mid-America Earthquake Center (MAE) headquartered at the University of Illinois at Urbana-Champaign.[53] All three centers support the work of geologists, engineers, and social scientists conducting research on earthquakes, earthquake resistant construction, and potential earthquake hazards. Review of the websites of these organizations and the materials contained therein provides a perspective on the current state of the art for mitigating hazards through engineering design.

After studying these resources, the prospective CIP instructor should be able to describe the different earth effects and natural disasters in both engineering and societal terms as well as articulate current efforts to quantify and understand these hazards and implement engineering and societal responses to them.

ANALYZING AND MANAGING RISK

RISK ANALYSIS

Risk analysis methodologies calculate a relative level of risk for an asset based on a set of criteria. One example of this is *Engineering Security: Protective Design for High Risk Buildings*, published by the New York City Police Department in 2009. It contains a methodology to rank major buildings into low, medium, and high hazards as well as limited design recommendations for high hazard facilities. A building's risk tier is determined based on threat, vulnerability, and impact and considers the following sub-categories, each rated as limited, moderate, or significant:

- Threat
  - Threat Profile
  - Target Attractiveness
- Vulnerability
  - Adjacency
  - Accessibility
  - Structural Performance
- Impact
  - Maximum Occupancy/Height
  - Economic Criticality
  - Transportation Criticality/Proximity
  - Critical Infrastructure Proximity

This process allows New York City to identify the highest hazard buildings within the metropolitan area. While it is useful for this purpose, it also highlights the shortcomings of relying solely on risk analysis. This method is only suitable under one set of specific conditions: large buildings located in an extremely large metropolitan area. Its measure of risk is both relative and qualitative and can only result in statements such as, "The risk to Building A is 'high' while the risk to Building C is 'low.'" Most importantly, it does not contain a methodology of directly evaluating the reduction in risk due to specific action and comparing the cost effectiveness of

competing risk reduction strategies.[54] To alleviate this shortcoming, one must progress beyond risk analysis to risk management.

RISK MANAGEMENT

Risk management involves the identification, consideration, selection, implementation, and continuous evaluation of risk mitigation strategies. It is begins with a risk analysis, but results in a changed, and hopefully improved, risk posture. Three risk management frameworks are presented here. In studying these frameworks, the potential CIP instructor will gain an appreciation of the principles of risk management and how they are applied in the context of different frameworks.

The Risk Management Series from FEMA is an ongoing effort to publish techniques, tools, and guidance to reduce the impact of threats and hazards to society and the built environment. All publications, along with several training courses, are available on the FEMA website at http://www.fema.gov/plan/prevent/rms/index.shtm#2. The *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, FEMA 426* is an excellent first reference for understanding counter-terrorism risk management. The six step process addresses the elements shown in Figure 4.

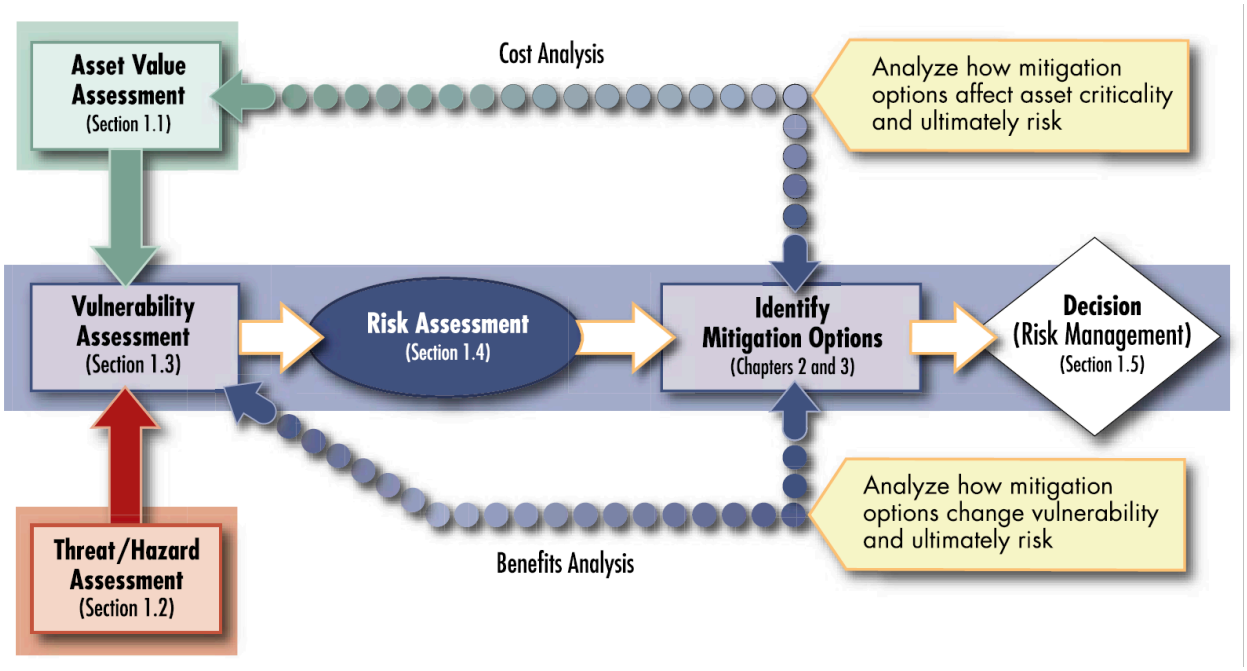

Figure 4. Risk Management Process of FEMA 426[55]

The asset valuation section considers a building's core functions, the individual infrastructure elements within the building, and the impact of the loss of each element. The Threat/Hazard Assessment section considers twelve different human caused threats to building elements but does not address natural hazards. The Vulnerability Assessment section considers site characteristics, population, and other factors to measure a building's vulnerability. Relative Risk is then assessed as a function of Asset Value, Threat Rating, and Vulnerability Rating for each asset or system against multiple different threats. High-risk areas are then targeted for mitigation using strategies

that address site layout, building design, blast resistance, and chemical, biological, and radiological considerations.[56]

The *Reference Manual* provides a comprehensive approach to risk management that is useful for professional self-development, application to actual projects, and classroom instruction. Its major limitations are that it is focused solely on buildings and the mitigation chapters address general strategies rather than specific design requirements.

Because of the scope of their construction program and real estate holdings as well as the threat of terrorist attack, the Department of Defense, has established a series of planning and design manuals that establish a minimum level of protection and a procedure for designing facilities that demonstrate a requirement for higher levels of protection. The baseline standard, detailed in UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, applies to all new and substantially renovated facilities and is focused on preventing mass casualty events. The risk management process, outlined in UFC 4-020-01, *DoD Security Engineering Facilities Planning Manual*, is very similar to the risk management process of FEMA 426 shown in Figure 4. The UFC 4-020-01 process considers a variety of assets within different facilities, relative values of these assets, multiple aggressor categories, and a wide array of aggressor tactics. Initial and adjusted levels of protection are selected based on asset value, threat likelihood, and effectiveness of protection. This manual also provides detailed design guidance on how to construct a facility to achieve a specific level of protection and the increase in cost above conventional construction,[57] which FEMA 426 does not do.

In addition to these two manuals, the UFC Security Engineering Series is a comprehensive set of manuals that covers many aspects of antiterrorism planning and design. The series is available online at the Whole Building Design Guide (www.wbdg.org). The WBDG is managed by the National Institute of Building Sciences and combines government criteria, non-government standards, research, and design guidance to achieve high-performance buildings.[58] The principle disadvantage of the UFC series is that some of the manuals are classified For Official Use Only (FOUO), meaning that their release is restricted to government agencies and selected contractors. Accordingly, this series is not generally recommended as a textbook or course reference where the FOUO material cannot be accessed.

While the New York City manual provides only risk analysis and FEMA 426 and UFC 4-020-01 focus on risk management for buildings, the risk management framework of the NIPP is a general process that can be applied to individual assets, systems, networks, and even entire infrastructure sectors. The framework is a closed loop process represented graphically in Figure 5. It has six steps and works across physical, cyber, and human dimensions.[59] Since it is a framework rather than a process or method, the NIPP describes what must be done in each step. How this is accomplished is left to the agency implementing the framework.

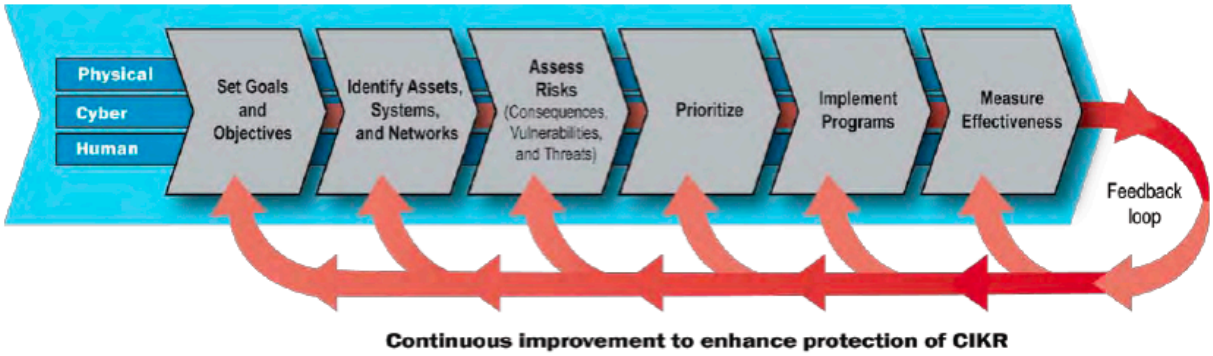

Figure 5. NIPP Risk Management Framework60

The NIPP Risk Management Framework has the advantage of being general enough to be applicable to almost any infrastructure asset. The accompanying disadvantage is that it lacks the detailed procedures to be applied to a specific infrastructure asset. It is essential for understanding and executing infrastructure protection in a general sense, but must be paired with detailed methodologies, research, and analysis for practical application. By applying this framework, CIP practitioners can relate a desired level of protection to an identified level of hazard, implement the programs to achieve the level of protection, and assess the effectiveness of the programs.

After studying the *Engineering Security: Protective Design for High Risk Buildings* process of risk analysis, the FEMA 426 and UFC 4-020-01 methods of risk management, and the NIPP Risk Management Framework, the prospective CIP instructor can differentiate between risk analysis and risk management, relate level of protection and level of hazard through a risk management process, and explain how risk management applies to infrastructure sectors at large.

FURTHER STUDIES IN RISK MANAGEMENT

While the procedures of FEMA 426 and UFC 4-020-01 work well when applied to buildings, they are not suitable under other conditions. To address risk in other infrastructure facilities and sectors, different methods are required. MSRAM, the Maritime Security Risk Analysis Model, is a tool used by the United States Coast Guard to assess and manage critical infrastructure risk in our nation's ports.[60] The Transit Risk Assessment Methodology (TRAM) arose from the efforts of the Port Authority of New York and New Jersey to develop a risk based funding allocation strategy for the protection of transportation assets and has since been used by many regional transportation authorities.[61] RAMCAP (Risk Analysis and Management for Critical Asset Protection) is a product of the American Society of Mechanical Engineers Innovative Technologies Institute (ASME-ITI). The current version, RAMCAP Plus, includes protection and resilience themes and can be applied to a wide range of facilities from college campuses to industrial facilities. ASME-ITI, together with the American Water Works Association (AWWA), has recently adapted the RAMCAP methodology to publish a new ANSI standard *J100 RAMCAP Risk and Resilience Management of Water and Wastewater Systems*.[62] Like FEMA 426 and UFC 4-020-01, these risk tools are appropriate for managing risk in discrete infrastructure elements and systems.

At the infrastructure sector level, the application of the NIPP Risk Management Framework can be seen in the thirteen currently published CIKR Sector Specific Plans. For example, the Dam Sector Specific Plan explains the Consequence-Based Top-Screen process used to conduct a sector wide risk assessment and program prioritization.[63] In contrast, the Water Sector Specific Plan applies the NIPP Risk Management Framework in the context of the Safe Drinking Water and Clean Water Acts to an infrastructure with over 160,000 individual systems that are locally owned and operated yet highly inter-dependent with other infrastructures.[64] Sector Specific Plans are also published for Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Defense Industrial Base, Energy, Information Technology, and National Monuments and Icons and demonstrate the application of the NIPP Risk Management Framework across different infrastructures.[65]

These are examples of actual risk management tools currently in use. While they might be too advanced for an introduction to risk course, they are certainly the standard for advanced courses and professional applications in CIP and risk management.

SYSTEM DESIGN

The design of protective systems is perhaps the broadest topic in the CIP conceptual framework and the course of investigation a prospective CIP instructor would naturally follow depends on program focus. However, a complete protective system encompasses physical, human, and cyber elements. The physical design of the facility tends to be the

province of engineers and architects while physical security or law enforcement professionals address the equipment and procedures employed by the personnel using and securing the facility. On top of these are the elements of cyber security, including information assurance, information security, and control and defense of SCADA (supervisory control and data acquisition) systems. A prospective CIP instructor does not need to be an expert in each of these fields but should have a general understanding of each and how they relate to one another. Basic information on these areas is readily available from a variety of open source resources and written in layman's terms. In studying these resources, the potential CIP instructor develops the ability to describe the processes, considerations, and design constraints necessary for a complete protective system.

THE PHYSICAL DIMENSION—DESIGN CONCEPTS FOR BUILDINGS

Buildings and the people, processes, and equipment they house are a component of every infrastructure system and they must be protected from terrorist attack and natural hazards. In many of these cases, particularly for human- and cyber-focused infrastructures, the purpose of the building is protection of the infrastructure. Therefore, all CIP professionals and educators should be familiar with the fundaments of building performance. The single best resource for gaining a conceptual understanding of protective design against a variety of threats and hazards is the resource page of the Whole Building Design Guide available at http://www.wbdg.org/resources/rpindex.php#.[66] The articles are prepared by a variety of professionals from different architectural and engineering firms and generally follow the format of Introduction, Description, Fundamentals, Applications, Relevant Codes and Standards, and Additional Resources. A recommended set of articles for gaining a conceptual understanding of protective design is included in Table 1 (below). Reading these articles does not make one an engineering design professional. Instead, the articles provide an understanding of how engineers and architects approach protective design and the difficulties in associated with this complex topic.

Table 1. Recommended Resources on the Whole Building Design Guide

General Category	Specific Topics
Terrorist Threats	Blast Safety of the Building Envelope
	Designing Buildings to Resist Explosive Threats
	Retrofitting Existing Buildings to Resist Explosive Threats
	Landscape Architecture and the Site Security Design Process
	The Site Security Design Process
	Windows and Glazing
Earth Effects& Natural Disasters	Flood Resistance of the Building Envelope
	Seismic Design Principles
	Seismic Safety of the Building Envelope
	Wind Safety of the Building Envelope
Planning	Balancing Security/Safety and Sustainability Objectives
	Cost Impact of the ISC Security Design Criteria
	Threat/Vulnerability Assessments and Risk Analysis
	UFC/ISC Security Design Criteria Overview and Comparison

Prospective CIP instructors in engineering programs are probably familiar with seismic, flood, and wind design procedures and may want to explore the technical aspects of blast design in more depth. Throughout the 1990s, conventional blast resistant design tended to focus on accidental explosions. Army Technical Manual (TM) 5-1300, *Structures to Resist the Effects of Accidental Explosions*, dated 1990 is a guide for protective design of facilities for the production, testing, storage, and demilitarization of explosive material.[67] Although TM 5-1300 is focused on accidental explosions rather terrorist acts, the science behind this document formed the basis for many current publications. *Design of Blast Resistant Buildings in Petrochemical Facilities*, published by the American Society of Civil Engineers in 1997, provides guidelines for the design of buildings subjected to accident explosion in petrochemical facilities. The progressive collapse of the Murrah Federal Building in Oklahoma City on April 19, 1995 and the events of September 11, 2001 resulted in protective design manuals focused on protecting structures and occupants from terrorist bombings. Structural design to prevent progressive collapse has been addressed by the American Institute of Steel Construction in *Blast and Progressive Collapse,*[68] and in the Unified Facilities Criteria 4-023-03 *Design of Buildings to Resist Progressive Collapse*.[69] The UFC series also addresses topics of electronic security systems, vehicle barriers, direct fire weapons effects, and airborne chemical, biological, and radiological protection. Finally, the American Society of Civil Engineers is developing a voluntary standard on *Blast Protection of Buildings* (expected to publish in 2011). These are technical design manuals that are only of interest to, and should only be employed by, engineering professionals.

After reviewing the materials through the Whole Building Design Guide, the prospective CIP instructor can describe the engineering, architectural, and site design approaches to hardening facilities against terrorist threats and natural disasters. Furthermore, the instructor can discuss the cost implications of increasing physical protection and the tradeoffs between security and other concerns including sustainability and accessibility. Prospective CIP instructors in engineering programs should also be familiar with current codes and standards for blast resistant construction and prevention of progressive collapse.

THE PHYSICAL DIMENSION — DESIGN CONCEPTS FOR OTHER PHYSICAL ELEMENTS

The resources for understanding the physical protection of buildings are robust and accessible at a non-technical level, primarily because everyone is familiar with, routinely uses, and is interested in the protection and resilience of where they live and work. The resources for other physical infrastructure sectors are somewhat harder to access because they are more specialized and require a greater level of technical expertise. In addition to the Sector Specific Plans, suggested references are presented here for three more physical infrastructure elements: dams, water resources, and electricity,

The Association of State Dam Safety Officials (ASDSO) is an organization of dam operators, owners, regulators, officials, and others interested in dam safety. Through education, training, standards, and outreach, their goal is to envision and achieve a future where all dams are safe. Their website, www.damsafety.org, provides excellent resources for anyone interested in dam safety, security, and resilience. The site provides links to dam owner manuals, inspection guides, safety standards, *The Journal of Dam Safety*, and links to other resources. There is also a tab for Infrastructure Security, which relates dam safety to the work of the Dams Sector done under DHS.[70]

A starting point for understanding water protection issues is the American Water Works Association (AWWA). Since 1881, AWWA has united educators, scientists, engineers, and operators to provide safe, sufficient, and protected water systems across North America. On the AWWA website (www.awwa.org), the Professional and Technical Resources tab contains standards, manuals of practice, assessment

tools, and management tools. Also available is the Water Infrastructure Security Enhancements (WISE) program, which is a joint program the American Society of Civil Engineers (ASCE) and the Water Environment Federation (WEF) that provides security guidelines and training materials for those who have a role in the physical protection of water infrastructure systems. This website also contains a link to purchase training on the *J100 RAMCAP Risk and Resilience Management of Water and Wastewater Systems* previously discussed.[71] AWWA has been one of the leaders and innovators in risk management of physical infrastructures and their work can inform and illuminate protection efforts for other infrastructures.

The nation's electrical system is a highly networked infrastructure with substantial physical, cyber, and operational security elements. A prospective CIP instructor without a background in electrical science, engineering, or operations might be tempted to completely shy away from this critical infrastructure, but a basic understanding of the functioning of the electrical system can be obtained through the use of several useful resources. *Electrical Power System Basics for the Nonelectrical Professional* by Steven W. Blume explains the elements of the electrical distribution system from generation to consumption conceptually and without complex mathematics.[72] The Department of Energy (DOE) website contains sections on Electricity 101, Smart Grid Primers, Fact Sheets, a Document Library, and an Interactive Grid demonstrating the interaction between generation, transmission, and consumption.[73] The DOE website and Blume's book provide a prospective CIP instructor with an understanding of system function without delving into detailed system and component design.

The North American Electric Reliability Corporation (NERC) operates under the auspices of Federal Energy Regulatory Commission (FERC) with the legal responsibility to enforce electrical reliability standards for power generators and distributors in the United States and Ontario and New Brunswick, Canada. The NERC website, www.nerc.com, contains reliability standards, reliability assessment data, and system performance trends for the North American electrical grid along with analysis of adverse electrical events. Because of their charge to maintain electrical reliability, NERC is responsible for many aspects of CIP in the electrical system and has published these nine CIP standards:[74]

CIP-001-1a	Sabotage Reporting
CIP-002-3	Cyber Security—Critical Cyber Asset Identification
CIP003-3	Cyber Security—Security Management Controls
CIP004-3	Cyber Security—Personnel and Training
CIP005-2a	Cyber Security— Electronic Security Perimeters
CIP006-3c	Cyber Security—Physical Security of Critical Cyber Assets
CIP007-3	Cyber Security—Systems Security Management
CIP008-3	Cyber Security—Incident Reporting and Response Planning
CIP009-3	Cyber Security—Recovery Plans for Critical Cyber Assets

The information on the NERC website is technically complex and may not be of interest to a prospective instructor in a general CIP course, but it would be essential in a detailed study of the reliability, resilience, and protection of the electrical grid.

These references provide a prospective CIP instructor with a fundamental understanding of protection in the dams, water, and electrical sectors. They also highlight the complexity of physical infrastructure protection and the need to engage with experts in each sector when detailed protective and resilient design is necessary. When needed, the same research

procedure can be used with other physical infrastructure elements. Begin with the sector specific plan then progress to professional and trade organizations operating in that sector. These organizations often supply information, training, and standards and – in many cases – are fully integrated with protection and resiliency efforts.

THE HUMAN DIMENSION – PROTECTIVE PERSONNEL AND PROCEDURES

Security and vulnerability analysis (SVA) is a tool that directly enables assessment of specifically identified threats to an organization (or its assets) and which identifies appropriate countermeasures. SVA can be considered an intellectual framework that includes the use of personnel and all organizational resources, the traditional "gates, guns and guards" of security. Like enterprise risk management (ERM), SVA is a continuous process, developed by the American Institute of Chemical Engineers (AIChE), of evaluating the effectiveness or adequacy of the personnel and procedures responsible for protecting a piece of critical infrastructure against identified hazards.[75] The overall intent of SVA is to identify and respond (a priori) to known or suspected security risks and to protect people, property, and the environment.

In an SVA, risk is a function of the product of the perceived likelihood of the hazard, the likelihood the threat could happen, and the severity of harm inflicted if the threat were to occur. Using this logic, all risks can be displayed in a risk matrix that facilitates their relative rankings assuming that no organization can afford to protect all their assets all the time from everything. Inasmuch as both ERM and SVA are disciplined processes designed to combine and correlate organizational strategy, personnel, resources (e.g., technology), and upper management in order to mitigate risk,[76] SVA is ultimately a process that operates as a component of ERM. In this way, SVA is a qualitative risk-based assessment tool that guides how organizations might address the likelihood of intentional acts of terrorism or other threats (e.g., natural disasters) that could result in loss or harm to the organization. The AIChE maintains a robust website regarding SVA within their Center for Chemical Process Safety (CCPS), which was developed following the Bhopal India disaster in 1984. The AIChE website (http://www.aiche.org/ccps/index.aspx) offers guidelines and networking, but it is not free.

As a component of the overall risk management approach within an organization, the principles surrounding SVA include continuous quality improvement and total organizational commitment. According to the CCPS, the core SVA process includes five steps:

1. Project planning
2. Facility characterization
3. Threat identification/assessment
4. Vulnerability analysis
5. Countermeasure identification/ selection

The CCPS model of SVA is elucidated as follows. Step 1 – Project Planning – entails the identification of an interdisciplinary team of security personnel and personnel directly tied to the piece of critical infrastructure the organization wishes to protect (i.e., the target assets). This team sets the objectives and scope of the SVA and begins to develop the security plan. Step 2 – Facility Characterization – includes several components including identification of the target assets and the technical details from each asset (e.g., the vulnerabilities of each asset and recommended methods of protecting those assets), specific identification of the hazards and their consequences were they to be realized to the assets (or the organization) including characterizing the target attractiveness, identification of existing security layers, and determination of the likelihood each threat presents including consequence analysis. Step 3 – Threat Assessment – considers all possible threats, both internal to the organization and external to the organization. Regarding human-based threats, the team would also attempt to characterize the presumed adversaries in terms of their capabilities and their characteristics. Working with local agencies (intelligence

agencies, weather bureaus, etc) is recommended. Step 4 – Vulnerability Analysis – matches each asset and the threat to that asset in order to elucidate the presumed vulnerability of that asset. The SVA team would also identify and incorporate any existing countermeasures and the degree to which such has been effective in reducing the vulnerability of the asset to date. By devising and discussing security-based scenarios, the SVA team can better evaluate the vulnerability of each asset vis-à-vis the identified threat. The SVA team should build a threat matrix in order to rank each threat and facilitate prioritization of risks. Step 5 is Countermeasure Identification/Selection. Selecting countermeasures is often difficult and needs to consider many competing organizational objectives. In the event current countermeasures are in place, the team would consider the consequences to the organization if those countermeasures fail or the layers of security are breached, and therefore, which additional or new countermeasures are required. In the event that no countermeasures are currently in place (say for example due the adoption of new technology or the construction of a new facility), the team would devise a set of countermeasures that would delay, reduce, mitigate, or prevent the threat from impacting the target asset.

Once completed, the SVA team generates a report for upper management. It is important to consider the cost benefit of all SVA generated recommendations. Generally speaking, if the vulnerability presents a lesser economic harm to the organization than the proposed solution, many organizations may decide to live with the vulnerability. Over time, the SVA team performs follow up (i.e., the continuous improvement portion) and determines adequacy of the implemented countermeasures or whether new vulnerabilities have arisen.

THE CYBER DIMENSION — ELECTRONIC SECURITY FUNDAMENTALS

Cyber Security is an incredibly complex area involving skilled professionals working in very specialized areas. At its core are efforts to protect and secure information and secure and defend control systems. The United States Computer Emergency Response Team (US-CERT) has the responsibility to protect the executive branch from cyber attacks and disseminate cyber security information to both other government agencies and the public;[77] it provides a good starting point for understanding cyber security.

Cyber systems process information – credit card numbers, bank accounts, birth records, and family photos. Information Assurance (IA) is a risk management process that protects the use, transmission, and storage of this information and the hardware and software that enable these processes. Fundamental IA concepts include confidentiality (information is disclosed only to authorized users), integrity (data is complete and correct), and availability (data is accessible when requested).[78] Formal education and training in information assurance is available at many institutions including over one hundred colleges and universities designated as National Security Agency Centers of Excellence.[79] The NSA-COE webpage provides links to these programs, some of which provide open source educational materials. One such site is the National Information Assurance Training and Education Center at the University of Idaho, which provides audio, video, text, and web-linked instructional materials on IA.[80]

SCADA systems are essential to the operation of the infrastructure. They allow operators in a centralized control facility to remotely operate pump stations, track movements of trains, monitor pressure in pipelines, and manage frequency and voltage in the electrical grid. Attacks on these systems can disable an infrastructure without physical contact and result in anything from complete destruction to no damage. One US-CERT effort to secure SCADA systems is the Control Systems Security Program (CSSP), which provides information, recommended practices, assessments, and training. Two useful web based training segments are "OPSEC for Control Systems," which teaches fundamentals of operations security as applied to SCADA systems, and "Cyber Security for Control Systems Engineers and Operators," which addresses cyber risk, threats, and mitigations as applied to modern control systems.[81] These training sessions each last about one hour and provide a

fundamental understanding of the importance of, and processes involved in, security SCADA systems.

These resources provide a prospective CIP instructor, regardless of background, with an understanding of the fundamentals of cyber security. These concepts must then be integrated with personnel and procedures and physical architectural and engineering design to provide a complete protective system for critical infrastructures.

EMERGENCE

The field of critical infrastructure protection is in a constant state of emergence. New threats and hazards arise each day and changes in demographics, society, and land use redefine old threats and the severity of existing hazards. CIP instructors and professionals must take a proactive approach to anticipating future developments. Some of these will come from predictable sources. For example, in March 2008, Toffler Associates assembled leaders of industry and government experts to address the most critical infrastructure challenges of the next fifteen years. The issues discussed included public-private sector coordination, asset concentration, infrastructure deterioration, foreign ownership, and cyber-interdependency.[82] Other perspectives on emergent issues may come from unexpected directions. The perception that the attacks of September 11, 2001 were "inconceivable" is false. In a 1995 bestselling novel, *Debt of Honor*, one of Tom Clancy's characters flew a 747 jumbo jet into the United States Capitol Building for the purpose of decapitating the U.S. Government. In the 1999 novel *Train Man*, P.T. Deutermann's protagonist sequentially destroys railroad bridges crossing the Mississippi River. Anyone with an understanding of the relationships between the rail, coal mining, and power infrastructures will quickly see that the potential infrastructure disruption of this kind of attack greatly exceeds the difficulties in Deutermann's plot. The world continues to change, visionaries still try to foresee the future, and we should assume our enemies read our novels. CIP educators and professionals must constantly remember the emergent state of our discipline and adapt accordingly.

CONCLUSION

Faculty expertise to develop and teach a college level course is traditionally developed through a combination of formal education and professional experience. Relying on this model in developing critical infrastructure protection education is not currently viable; it will not produce enough instructors fast enough to meet the educational demands of either students or employers in the homeland security field. The large number of homeland security and engineering programs currently lacking critical infrastructure protection courses is evidence of this. One solution is to grow the instructor base through instructor self-education using the outline provided in this paper. This guide directs a faculty member with expertise in a field related to CIP to the resources necessary to acquire sufficient breadth and depth of knowledge to teach an introductory course in CIP. The resources further provide a foundation for the deeper study necessary for more advanced courses. At the completion of this self-study, the prospective CIP instructor will, to a depth appropriate to the instructor's and the institution's specialization and mission, be able to:

1. Explain national strategies and policies on infrastructure protection;
2. Identify critical components of a complex infrastructure network;
3. Describe the All Hazards Environment for these critical components;
4. Specify the level of protection or resiliency for these critical components;
5. Describe systems design concepts to achieve the desired protection and resiliency.

Building on this foundation, the new CIP instructor can then explore particular topics in greater depth.

The ultimate purpose in engaging in this course of self-study is to develop and teach a CIP course. The conceptual framework for

understanding and assimilating CIP information presented in this paper – Policy, Networks, All-Hazards, Level of Threat, Level of Protection, and System Design – is also useful for organizing a course and forms the basic blocks of instruction in an introductory CIP course. The knowledge gained by the new CIP instructor can now be translated into lesson titles, lesson objectives, reading assignments, learning activities, course notes, projects, and homework. Through this process both the ranks of CIP instructors and the quality and quantity of critical infrastructure protection courses can grow to meet the demands of both homeland security students and professionals.

About The Authors

Steven D. Hart *is a Lieutenant Colonel in the United States Army Corps of Engineers with over twenty-two years of service in both command and staff positions in Iraq, Kuwait, Panama, Germany, Korea, and the United States. He is currently assigned as an assistant professor in the Department of Civil and Mechanical Engineering at West Point where he is teaching innovative courses on infrastructure engineering and critical infrastructure protection.*

Jim Ramsay *is the coordinator of the homeland security undergraduate program at Embry-Riddle Aeronautical University and currently serves on the CDC/NIOSH Board of Scientific Counselors and the ABET Board of Directors, and as the accreditation coordinator for the Homeland Security Defense Education Consortium Association. Dr. Ramsay has developed and taught courses in terrorism, risk management and critical infrastructure, emergency management, exercise design and evaluation. His research areas include environmental security and its relationship to national security, emergency management effectiveness and resilience. Dr. Ramsay may be contacted at ramsa301@erau.edu.*

[1] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: Wiley-Interscience, 2006).

[2] Ibid.

[3] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: DHS, 2009), 109 and 19.

[4] Center for Homeland Defense and Security (CHDS), http://www.chds.us/, and About CHDS tab, http://www.chds.us/?about.

[5] Homeland Security Education University and Agency Partnership homepage, http://www.chds.us/?special/info&pgm=Partner and the secure log on: https://www.chds.us/courses/course/view.php?id=322.

[6] Center for Homeland Defense and Security self study course webpage, http://www.chds.us/courses/

[7] About HSDL (Homeland Security Digital Library), http://www.hsdl.org/?about

[8] CHDS Educational Resources page, (https://www.chds.us/?chds:innovations#

[9] Critical Infrastructure Protection Program, George Mason University, http://cip.gmu.edu/

[10] Center for Infrastructure Protection and Physical Security, http://cipps.eng.ufl.edu/site/

[11] Ted Krauthammer, *Modern Protective Structures* (CRC Press, 2008).

[12] Institute for Crisis, Disaster, and Risk Management, George Washington University, http://www.gwu.edu/~icdrm/index.html

[13] Carleton University, MIPIS Information Brochure, http://www2.carleton.ca/graduate-studies/ccms/wp-content/ccms-files/MIPIS.pdf

[14] Benjamin Bloom, editor, *Taxonomy of Educational Objectives: Handbook I: Cognitive Domain* (David McKay Company, Inc, 1956).

[15] FEMA EMI website, IS860.a course home page, http://training.fema.gov/EMIWeb/IS/is860a.asp .

[16] 107th Congress, Public Law 107-296, http://www.cio.gov/documents/pl_107_296_nov_25_2003.pdf .

[17] Homeland Security Presidential Directive 7 (2003), http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

[18] Homeland Security Presidential Directive 8 (2003), http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

[19] Homeland Security Presidential Directive 5 (2003), http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm .

[20] National Strategy for Homeland Security, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (2007).

[21] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003), http://www.dhs.gov/files/publications/publication_0017.shtm.

[22] DHS Sector Specific Plans website, http://www.dhs.gov/files/programs/gc_1179866197607.shtm#2.

[23] FEMA NRF Resource Center, http://www.fema.gov/emergency/nrf/.

[24] FEMA NIMS Resource Center http://www.fema.gov/emergency/nims/ .

[25] Albert-László Barabási and Eric Bonabeau, "Scale Free Networks," *Scientific America* (May 2003), http://www.scientificamerican.com/article.cfm?id=scale-free-networks

[26] M.E.J Newman, "The Structure and Function of Complex Networks" *SIAM Review* 45 (2003): 67, http://www-personal.umich.edu/~mejn/courses/2004/cscs535/review.pdf

[27] Lewis, *Critical Infrastructure Protection in Homeland Security*.

[28] Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University, http://www.casos.cs.cmu.edu/projects/ora/index.html.

[29]Interdisciplinary Center for Network Science and Application, University of Norte Dame, http://icensa.nd.edu/.

[30]DHS Website, http://www.dhs.gov/files/programs/gc_1217445858859.shtm.

[31] *National Infrastructure Protection Plan* (Department of Homeland Security, 2009), 110.

[32] UFC 4-020-01 *DoD Security Engineering Facilities Planning Manual,* Glossary (2008), 8.

[33] Ibid.

[34] *National Infrastructure Protection Plan*, 109.

[35] Second Vatican Council, *GAUDIUM ET SPES (JOYS AND HOPES)* (Pastoral Constitution on the Church in the Modern World, 1965).

[36] DCSINT, US ARMY TRADOC, *A Military Guide To Terrorism In The Twenty First Century, Handbook 1*. (Fort Leavenworth, KS,: 2007).

[37] DCSINT, US ARMY TRADOC, *Terror Operations Case Studies in Terrorism, Handbook 1.01*. (Fort Leavenworth KS: 2007).

[38] DCSINT, US ARMY TRADOC, *Critical Infrastructure Threats and Terrorism, Handbook 1.02* (Fort Leavenworth KS: 2006).

[39] U.S. Department of State, Office of The Coordinator For Counterterrorism, http://www.state.gov/s/ct/.

[40] FBI Counterterrorism home page http://www.fbi.gov/terrorinfo/counterrorism/waronterrorhome.htm.

[41] National Counterterrorism Center, http://www.nctc.gov/.

[42] CIA Center for the Study of Intelligence, https://www.cia.gov/library/center-for-the-study-of-intelligence/index.html.

[43] National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland, http://www.start.umd.edu/start/.

[44] Memorial Institute for the Prevention of Terrorism, http://www.mipt.org/.

[45] Combating Terrorism Center, United States Military Academy, http://www.ctc.usma.edu/.

[46] Natural Hazards Gateway, http://www.usgs.gov/hazards/.

[47] Natural Hazards—Flood page, http://pubs.usgs.gov/fs/2006/3026/ .

[48] Natural Hazards Support System, http://nhss.cr.usgs.gov/.

[49] Natural Hazards Center Homepage, http://www.colorado.edu/hazards/.

[50] The Department of Homeland Security Center of Excellence—Natural Disasters, Coastal Infrastructure and Emergency Management, http://hazardscenter.unc.edu/diem/index.php.

[51] Pacific Earthquake Engineering Research Center, http://peer.berkeley.edu/.

[52] Mid-Continent Earthquake Engineering Research Center, http://mceer.buffalo.edu/.

[53] Mid-America Earthquake Center, http://mae.cee.uiuc.edu/.

[54] New York City Police Department, *Engineering Security: Protective Design for High Risk Buildings* (2009), http://www.nyc.gov/html/nypd/html/counterterrorism/engineeringsecurity.shtml.

[55] FEMA, *Reference Manual to Mitigate Potential Terrorist Attack Against Buildings*, figure 1-3 (Washington, DC: FEMA, 2003), 1-5.

[56] Ibid.

[57] U.S. Department of Defense, *DoD Security Engineering Facilities Planning Manual* UFC 4-020-01 (Washington, DC: DoD, 2008).

[58] Whole Building Design Guide, http://www.wbdg.org/wbdg_ug.php#hide.

[59] *National Infrastructure Protection Plan*, chapter 3.

[60] MSRAM Brochure, http://aapa.files.cms-plus.com/PDFs/MSRAMBrochureTrifold.pdf.

[61] Security Analysis and Risk Management Association, *Transit Risk Assessment Methodology (TRAM)*, http://www.sarma-wiki.org/index.php?title=Transit_Risk_Assessment_Methodology_(TRAM).

[62] American Society of Mechanical Engineers—Innovative Technologies Institute, RAMCAP Plus Process Home Page, http://www.asme-iti.org/RAMCAP/RAMCAP_Plus_2.cfm.

[63] DHS, *Dam Sector Specific Plan* (2010), http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf.

[64] DHS, *Water Sector Specific Plan* (2007), http://www.dhs.gov/xlibrary/assets/nipp-ssp-water.pdf.

[65] Sector Specific Plans page, DHS website: http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

[66] The Resources Page on the Whole Building Design Guide cannot be accessed through a tab. It must be accessed either by using the link provided in the text or by navigating through the site map to a particular resource topic.

[67] Army Technical Manual 5-1300, *Structures to Resist the Effects of Accidental Explosions*, (U.S. Army: 1990), http://www.ddesb.pentagon.mil/tm51300.htm

[68] Kirk A. Marchand and Farid Alfawakhiri, *Blast and Progressive Collapse* (AISC, 2004) http://www.aisc.org/WorkArea/showcontent.aspx?id=7042.

[69] American Institute of Steel Construction, *Design of Buildings to Resist Progressive Collapse with Change 1,* UFC (United Facilities Criteria) 4-023-03 (2009).

[70] Association of State Dam Safety Officials website: http://www.damsafety.org/.

[71] American Water Works Association website accessed at http://www.awwa.org/index.cfm .

[72] Steven W. Blume, *Electrical Power System Basics for the Nonelectrical Professional* (Piscataway: Wiley-Interscience and IEEE Press, 2007).

[73] Department of Energy Website: http://www.oe.energy.gov/information_center/electricity101.htm.

[74] North American Electrical Reliability Corporation website, Standards page, http://www.nerc.com/page.php?cid=2%7C20 .

[75] AIChE Security and Vulnerability Analysis, Course 622, http://www.aiche.org/education.

[76] K.M. Hess, *Introduction to Private Security*, 5th ed. (Wadsworth Press, 2009).

[77] US-CERT homepage: http://www.us-cert.gov/aboutus.html.

[78] Wikipedia, "Information Assurance," http://en.wikipedia.org/wiki/Information_assurance.

[79] National Security Agency Center of Excellence web page: http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

[80] National Information Assurance Training and Education Center web page: http://niatec.info/ViewPage.aspx?id=0.

[81] US-CERT CSSP training homepage: http://www.us-cert.gov/control_systems/cstraining.html.

[82] Toffler Associates, "Five Critical Infrastructure Threats," http://www.toffler.com/docs/Five-Critical-Infrastructure-Threats.pdf.